

A note on linear Sperner families

Gábor Hegedűs*, Lajos Rónyai†

February 3, 2017

This paper is dedicated to the memory of our teacher, colleague and friend, professor Tamás E. Schmidt.

Abstract

In an earlier work we described Gröbner bases of the ideal of polynomials over a field, which vanish on the set of characteristic vectors $\mathbf{v} \in \{0, 1\}^n$ of the complete d uniform set family over the ground set $[n]$. In particular, it turns out that the standard monomials of the above ideal are *ballot monomials*. We give here a partial extension of this fact. A set family is a *linear Sperner system* if the characteristic vectors satisfy a linear equation $a_1v_1 + \dots + a_nv_n = k$, where the a_i and k are positive integers. We prove that the lexicographic standard monomials for linear Sperner systems are also ballot monomials, provided that $0 < a_1 \leq a_2 \leq \dots \leq a_n$. As an application, we confirm a conjecture of Frankl in the special case of linear Sperner systems.

2010 AMS Subject classification: Primary: 13P25; Secondary: 13P10, 05D05.

Key words and phrases: Sperner family, characteristic vector, polynomial function, Gröbner basis, standard monomial, ballot monomial, shattering.

⁰Research supported in part by National Research, Development and Innovation Office - NKFIH Grant No. K115288.

*Óbuda University, Antal Bejczy Center for Intelligent Robotics, Kiscelli utca 82, Budapest, Hungary, H-1032, hegedus.gabor@nik.uni-obuda.hu

†Institute of Computer Science and Control, Hungarian Academy of Sciences; Department of Algebra, Budapest University of Technology, Budapest, lajos@info.ilab.sztaki.hu

1 Introduction

Throughout the paper n will be a positive integer and $[n]$ stands for the set $\{1, 2, \dots, n\}$. The family of all subsets of $[n]$ is denoted by $2^{[n]}$.

Let \mathbb{F} be a field. $\mathbb{F}[x_1, \dots, x_n] = \mathbb{F}[\mathbf{x}]$ denotes the ring of polynomials in commuting variables x_1, \dots, x_n over \mathbb{F} . For a subset $F \subseteq [n]$ we write $\mathbf{x}_F = \prod_{j \in F} x_j$. In particular, $\mathbf{x}_\emptyset = 1$.

Let $\mathbf{v}_F \in \{0, 1\}^n$ denote the characteristic vector of a set $F \subseteq [n]$. For a family of subsets $\mathcal{F} \subseteq 2^{[n]}$, let $V(\mathcal{F}) = \{\mathbf{v}_F : F \in \mathcal{F}\} \subseteq \{0, 1\}^n \subseteq \mathbb{F}^n$. A polynomial $f \in \mathbb{F}[x_1, \dots, x_n]$ can be considered as a function from $V(\mathcal{F})$ to \mathbb{F} in the straightforward way.

Several interesting properties of finite set systems $\mathcal{F} \subseteq 2^{[n]}$ can be formulated simply as statements about *polynomial functions on $V(\mathcal{F})$* . For instance, the rank of certain inclusion matrices can be studied in this setting (see for example Sections 2, 3 in [14]). As for polynomial functions on $V(\mathcal{F})$, it is natural to consider the ideal $I(V(\mathcal{F}))$:

$$I(V(\mathcal{F})) := \{f \in \mathbb{F}[\mathbf{x}] : f(\mathbf{v}) = 0 \text{ whenever } \mathbf{v} \in V(\mathcal{F})\}.$$

Substitution gives an \mathbb{F} algebra homomorphism from $\mathbb{F}[\mathbf{x}]$ to the \mathbb{F} algebra of \mathbb{F} -valued functions on $V(\mathcal{F})$. A straightforward interpolation argument shows that this homomorphism is surjective, and the kernel is exactly $I(V(\mathcal{F}))$. This way we can identify $\mathbb{F}[\mathbf{x}]/I(V(\mathcal{F}))$ and the algebra of \mathbb{F} valued functions on $V(\mathcal{F})$. As a consequence, we have

$$\dim_{\mathbb{F}} \mathbb{F}[\mathbf{x}]/I(V(\mathcal{F})) = |\mathcal{F}|. \quad (1)$$

Gröbner bases and related structures of $I(V(\mathcal{F}))$ were given for some families \mathcal{F} , see [14] and the references therein. Before proceeding further, we recall some basic facts about Gröbner bases and standard monomials. For details we refer to [1], [5], [6], [7].

A linear order \prec on the monomials over variables x_1, x_2, \dots, x_m is a *term order*, or *monomial order*, if 1 is the minimal element of \prec , and $\mathbf{u}\mathbf{w} \prec \mathbf{v}\mathbf{w}$ holds for any monomials $\mathbf{u}, \mathbf{v}, \mathbf{w}$ with $\mathbf{u} \prec \mathbf{v}$. Two important term orders are the lexicographic order \prec_l and the deglex order \prec_d . We have

$$x_1^{i_1} x_2^{i_2} \cdots x_m^{i_m} \prec_l x_1^{j_1} x_2^{j_2} \cdots x_m^{j_m}$$

iff $i_k < j_k$ holds for the smallest index k such that $i_k \neq j_k$. Concerning the deglex order, we have $\mathbf{u} \prec_d \mathbf{v}$ iff either $\deg \mathbf{u} < \deg \mathbf{v}$, or $\deg \mathbf{u} = \deg \mathbf{v}$, and $\mathbf{u} \prec_l \mathbf{v}$.

The *leading monomial* $\text{lm}(f)$ of a nonzero polynomial $f \in \mathbb{F}[\mathbf{x}]$ is the \prec -largest monomial which appears with nonzero coefficient in the canonical form of f as a linear combination of monomials.

Let I be an ideal of $\mathbb{F}[\mathbf{x}]$. A finite subset $G \subseteq I$ is a *Gröbner basis* of I if for every nonzero $f \in I$ there exists a $g \in G$ such that $\text{lm}(g)$ divides $\text{lm}(f)$. In other words, the leading monomials $\text{lm}(g)$ for $g \in G$ generate the semigroup ideal of monomials $\{\text{lm}(f) : f \in I\}$. It follows easily, that G is actually a basis of I , i.e. G generates I as an ideal of $\mathbb{F}[\mathbf{x}]$. A key fact is (cf. [6, Chapter 1, Corollary 3.12] or [1, Corollary 1.6.5, Theorem 1.9.1]) that every nonzero ideal I of $\mathbb{F}[\mathbf{x}]$ has a Gröbner basis.

A monomial $\mathbf{w} \in \mathbb{F}[\mathbf{x}]$ is a *standard monomial for I* if it is not a leading monomial for any $f \in I$. We denote by $\text{sm}(I)$ the set of standard monomials of I . For a nonzero ideal I of $\mathbb{F}[\mathbf{x}]$ the set of monomials $\text{sm}(I)$ is a downset: if $\mathbf{w} \in \text{sm}(I)$, \mathbf{u}, \mathbf{v} are monomials from $\mathbb{F}[\mathbf{x}]$ such that $\mathbf{w} = \mathbf{u}\mathbf{v}$ then $\mathbf{u} \in \text{sm}(I)$. Also, $\text{sm}(I)$ gives a basis of the \mathbb{F} -vectorspace $\mathbb{F}[\mathbf{x}]/I$ in the sense that every polynomial $g \in \mathbb{F}[\mathbf{x}]$ can be uniquely expressed as $h + f$ where $f \in I$ and h is a unique \mathbb{F} -linear combination of monomials from $\text{sm}(I)$.

For a set family $\mathcal{F} \subseteq 2^{[n]}$ the characteristic vectors in $V(\mathcal{F})$ are all 0,1-vectors, hence the polynomials $x_i^2 - x_i$ all vanish on $V(\mathcal{F})$. We infer that the standard monomials of $I(\mathcal{F}) := I(V(\mathcal{F}))$ are square-free monomials. Moreover, (1) and the preceding paragraph imply that

$$|\mathcal{F}| = \dim_{\mathbb{F}} \mathbb{F}[\mathbf{x}]/I(\mathcal{F}) = |\text{sm}(I(\mathcal{F}))|. \quad (2)$$

Let $\mathbf{a} = (a_1, \dots, a_n)$ be a vector with positive integer components a_i , and $k \in \mathbb{N}$. We define the set of vectors $S(\mathbf{a}, k) \subseteq \{0, 1\}^n \subseteq \mathbb{F}^n$ as follows:

$$S(\mathbf{a}, k) := \{(v_1, \dots, v_n) \in \{0, 1\}^n : \sum_{i=1}^n a_i v_i = k\}.$$

In this paper, with the exception of a brief remark, where $\mathbb{F} = \mathbb{F}_p$ is considered, we assume that $\mathbb{F} = \mathbb{Q}$. The set family corresponding to $S(\mathbf{a}, k)$ is a Sperner system or antichain. Sperner systems of the form $S(\mathbf{a}, k)$ are called *linear Sperner systems*. There are Sperner systems which are non linear. A simple example is the following family:

$$T := \{(1, 1, 0, 0, 0), (1, 0, 1, 0, 0), (1, 0, 0, 1, 0), (1, 0, 0, 0, 1), (0, 1, 1, 0, 0), (0, 0, 1, 1, 1)\}.$$

Indeed, easy linear algebra shows that $S(\mathbf{a}, k)$ can contain the first 5 points of T only if $a_1 = a_2 = \dots = a_5$.

The complete uniform family of all d element subsets of $[n]$ is linear, in fact it is $S(\mathbf{1}, d)$, where $\mathbf{1} = (1, \dots, 1)$. Following [2], in [11] we described Gröbner bases and standard monomials for the ideals $I_{n,d} = I(S(\mathbf{1}, d))$. Extensions and combinatorial applications were given in [12].

Assume that \prec is an arbitrary term order on $\mathbb{F}[\mathbf{x}]$ such that $x_1 \succ x_2 \succ \dots \succ x_n$. Let $0 \leq d \leq n/2$ and denote by $\mathcal{M}_{d,n}$ the set of all monomials \mathbf{x}_G such that $G = \{s_1 < s_2 < \dots < s_j\} \subset [n]$ for which $j \leq d$ and $s_i \geq 2i$ holds for every i , $1 \leq i \leq j$. These monomials \mathbf{x}_G are the *ballot monomials* of degree at most d . If n is clear from the context, then we write \mathcal{M}_d instead of the more precise $\mathcal{M}_{d,n}$. It is known (see for example Lemma 2.3 and the following remark in [2]) that

$$|\mathcal{M}_d| = \binom{n}{d}.$$

In [2] it was also shown for the lex order \prec_l , and this was extended in [11] to any term order \prec such that $x_n \prec \dots \prec x_1$, that \mathcal{M}_d is the set of standard monomials for $I_{n,d}$ as well as for $I_{n,n-d}$. Our main aim in this note is to prove a partial extension of the above result to linear Sperner systems. Some of the results in [4] also served as motivation for our work in this direction.

Theorem 1.1 *Let $\mathbf{a} = (a_1, \dots, a_n) \in \mathbb{Z}^n$ be a vector such that $0 < a_1 \leq a_2 \leq \dots \leq a_n$, and k be a natural number. Then the lexicographic standard monomials for $S(\mathbf{a}, k)$ are all ballot monomials. More precisely*

$$\text{sm}(I(S(\mathbf{a}, k))) \subseteq \mathcal{M}_{\lfloor n/2 \rfloor}.$$

In the following example we give an explicit description of the lex standard monomials for $S(\mathbf{a}, k)$, when $a_1 = \dots = a_{n-1} = 1$, and $a_n = t$ for some integer $t \geq 1$.

Example 1 *Let $1 \leq t \leq k \leq \frac{n-1}{2}$ be integers, $a_1 = \dots = a_{n-1} = 1$, $a_n := t$, and put $V := S(\mathbf{a}, k)$. Then the set of the lex standard monomials of $I(V)$ is*

$$\text{sm}(I(V)) = \mathcal{M}_{k,n-1} \cup \{\mathbf{m}x_n : \mathbf{m} \in \mathcal{M}_{k-t,n-1}\}.$$

The following fact is easy to see by symmetric chain decomposition (see Problem 13.20 in [13]). Here we offer a somewhat algebraic proof.

Corollary 1.2 *Suppose that the coordinates of $\mathbf{a} \in \mathbb{Z}^n$ are positive integers and $k \leq \frac{n}{2}$ is a natural number. Then*

$$|S(\mathbf{a}, k)| \leq \binom{n}{k}.$$

Proof. After possibly permuting the coordinates, we may assume that $0 < a_1 \leq a_2 \leq \dots \leq a_n$. Observe also that a monomial \mathbf{x}_G is a leading monomial for $I(S(\mathbf{a}, k))$ whenever $|G| > k$, hence

$$|S(\mathbf{a}, k)| = |\text{sm}(I(S(\mathbf{a}, k)))| \leq |\mathcal{M}_k| = \binom{n}{k}.$$

Here we first used (2), and the inequality follows from Theorem 1.1. \square

A set family $\mathcal{F} \subseteq 2^{[n]}$ *shatters* a subset $S \subseteq [n]$, if for every $Y \subseteq S$ there exists an $F \in \mathcal{F}$ such that $F \cap S = Y$. In [9] Frankl conjectured that if a Sperner system $\mathcal{F} \subseteq 2^{[n]}$ does not shatter any ℓ element subset of $[n]$ for some integer $0 \leq \ell \leq n/2$, then

$$|\mathcal{F}| \leq \binom{n}{\ell-1}.$$

Here we confirm this conjecture for linear Sperner systems.

Corollary 1.3 *Suppose that the coordinates of $\mathbf{a} \in \mathbb{Z}^n$ are positive integers, k, ℓ are natural numbers, $\ell \leq n/2$, and $S(\mathbf{a}, k)$ does not shatter any ℓ element subset of $[n]$. Then*

$$|S(\mathbf{a}, k)| \leq \binom{n}{\ell-1}.$$

Proof. After possibly permuting coordinates, we may again assume that $0 < a_1 \leq a_2 \leq \dots \leq a_n$. By Theorem 1.1 the lex standard monomials of $S(\mathbf{a}, k)$ are ballot monomials. Next we observe that the square-free monomials of degree at least ℓ are leading monomials for $S(\mathbf{a}, k)$. Indeed, let $S \subseteq [n]$ be a subset, $|S| \geq \ell$. Then S is not shattered by $S(\mathbf{a}, k)$: there is a subset $Y \subseteq S$ such that no $F \subseteq [n]$ for which $\mathbf{v}_F \in S(\mathbf{a}, k)$ can give $Y = S \cap F$. Then the polynomial

$$f(\mathbf{x}) = \prod_{i \in Y} x_i \cdot \prod_{j \in S \setminus Y} (x_j - 1)$$

vanishes on $S(\mathbf{a}, k)$ completely, and the leading monomial of f is \mathbf{x}_S (for an arbitrary term order). We obtain that

$$\text{sm}(I(S(\mathbf{a}, k))) \subseteq \mathcal{M}_{\ell-1},$$

and hence

$$|S(\mathbf{a}, k)| = |\text{sm}(I(S(\mathbf{a}, k)))| \leq |\mathcal{M}_{\ell-1}| = \binom{n}{\ell-1}.$$

□

Let p be a prime, $\mathbf{a} \in \mathbb{N}^n$ be a vector, $k \in \mathbb{N}$. We consider the family

$$S_p(\mathbf{a}, k) = \{\mathbf{v} \in \{0, 1\}^n : \sum_{i=1}^n a_i v_i \equiv k \pmod{p}\} \subset \mathbb{Q}^n.$$

Note that $S_p(\mathbf{a}, k)$ is no longer a Sperner family. An interesting and useful fact is (see [10], [12]) that in degrees at most $p-1$ the deglex standard monomials for $S(\mathbf{1}, k)$ and $S_p(\mathbf{1}, k)$ are the same over \mathbb{F}_p . We have a similar but weaker statement for more general \mathbf{a} . Weaker in the sense that stronger upper bound is required for the degree of the monomials, and also in the sense that our argument works only for lex standard monomials¹.

Let t be an integer, $0 < t \leq n/2$. We define \mathcal{H}_t as the set of those subsets $\{s_1 < s_2 < \dots < s_t\}$ of $[n]$ for which t is the smallest index j with $s_j < 2j$.

We have $\mathcal{H}_1 = \{\{1\}\}$, $\mathcal{H}_2 = \{\{2, 3\}\}$, and $\mathcal{H}_3 = \{\{2, 4, 5\}, \{3, 4, 5\}\}$. It is clear that if $\{s_1 < \dots < s_t\} \in \mathcal{H}_t$, then $s_t = 2t - 1$, and $s_{t-1} = 2t - 2$ if $t > 1$.

Proposition 1.4 *Suppose that $0 < a_i \leq a_{i+1}$ for each $1 \leq i \leq n-1$. Let $0 < t \leq n/2$ be an integer, $T \in \mathcal{H}_t$, and assume that $\sum_{i \in T} a_i < p$. Then \mathbf{x}_T is a lex leading monomial for $S_p(\mathbf{a}, k)$. In particular, the conclusion holds when $\sum_{i \in [2t-1]} a_i \leq p$.*

In the next Section we prove Theorem 1.1, Proposition 1.4, and discuss the details of Example 1.

¹A set $V \subseteq \{0, 1\}^n$ can be considered as a subset of \mathbb{F}^n for any field \mathbb{F} . It is known that the set of lex standard monomials for $I(V)$ is independent of \mathbb{F} . This is seen for example from Proposition 2.3.

2 Lex standard monomials for linear Sperner systems

We shall need the following simple observations.

Fact 2.1 *Let $G \subseteq [n]$. If the monomial \mathbf{x}_G is not a ballot monomial, then there exists an integer $t > 0$ and a $Y \in \mathcal{H}_t$ such that $Y \subseteq G$. \square*

Lemma 2.2 *Let $0 < a_1 \leq a_2 \leq \dots \leq a_n$ and t be integers, $1 < t \leq n/2$, $T \in \mathcal{H}_t$. Then*

$$\sum_{i \in [2t-1] \setminus T} a_i \leq \sum_{i \in T \setminus \{2t-1\}} a_i < \sum_{i \in T} a_i.$$

Proof. We prove that there exists a bijective map f from $T \setminus \{2t-1\}$ onto $[2t-1] \setminus T$ such that $f(t) < t$ for every $t \in T \setminus \{2t-1\}$.

This holds because $T \in \mathcal{H}_t$ and therefore if

$$T \setminus \{2t-1\} = \{l_1 < l_2 < \dots < l_{t-1}\},$$

then $l_i \geq 2i$ for $i = 1, \dots, t-1$. The map f can be constructed inductively for l_1, \dots, l_{t-1} .

Indeed, we can set $f(l_1) = 1$. Suppose now that we have constructed $f(l_j)$ for $j < i$. The numbers l_j and $f(l_j)$ are all positive integers less than l_i by the induction hypothesis. Their number is $2i-2$. In the interval $[1, 2i-1]$ there are $2i-1$ integers, hence we have one, say s , which is not among the numbers considered previously. Then we can set $f(l_i) = s$.²

The existence of f implies that

$$\sum_{i \in [2t-1] \setminus T} a_i \leq \sum_{i \in T \setminus \{2t-1\}} a_i < \sum_{i \in T} a_i.$$

This proves the lemma. \square

²An alternative way to construct f is to observe first that if we write

$$\{1, 2, \dots, 2t-2\} = \{l_1 < l_2 < \dots < l_{t-1}\} \cup^* \{s_1 < s_2 < \dots < s_{t-1}\},$$

then we have $s_i < l_i$ for $i = 1, \dots, t-1$. We can then set $f(l_i) = s_i$ for every i .

Following [8] and [14] we recall some facts about the Lex game, a method to determine the lexicographic standard monomials of the vanishing ideal of a finite set of points from \mathbb{F}^n , where \mathbb{F} is an arbitrary field. Let $V \subseteq \mathbb{F}^n$ be a finite set, and $\mathbf{w} = (w_1, \dots, w_n) \in \mathbb{N}^n$ an n dimensional vector of natural numbers. With these data as parameters, we define the Lex game $\text{Lex}(V; \mathbf{w})$, which is played by two players, Lea and Stan, as follows: Both Lea and Stan know V and \mathbf{w} . Their moves are:

1 Lea chooses w_n elements of \mathbb{F} .

Stan picks a value $y_n \in \mathbb{F}$, different from Lea's choices.

2 Lea now chooses w_{n-1} elements of \mathbb{F} .

Stan picks a $y_{n-1} \in \mathbb{F}$, different from Lea's (last w_{n-1}) choices.

... (The game proceeds in this way until the first coordinate.)

n Lea chooses w_1 elements of \mathbb{F} .

Stan finally picks a $y_1 \in \mathbb{F}$, different from Lea's (last w_1) choices.

The winner of the game is Stan, if in the course of the game he can select a vector $\mathbf{y} = (y_1, \dots, y_n)$ such that $\mathbf{y} \in V$, otherwise Lea wins the game. If in any step there is no suitable choice y_i for Stan, then Lea wins also.

The game allows a characterization of the lexicographic leading monomials and standard monomials for V (Theorems 2 and 3 in [8]).

Proposition 2.3 *Let $V \subseteq \mathbb{F}^n$ be a nonempty finite set and $\mathbf{w} \in \mathbb{N}^n$. Stan wins $\text{Lex}(V; \mathbf{w})$ if and only if $\mathbf{x}^{\mathbf{w}}$ is a lex standard monomial for $I(V)$. Equivalently, Lea wins the lex game if and only if $\mathbf{x}^{\mathbf{w}}$ is a lex leading monomial for the ideal $I(V)$.*

Proof of Theorem 1.1. We may assume that $S = S(\mathbf{a}, k)$ is nonempty. By Fact 2.1 it suffices to prove that for any integer $1 \leq t \leq n/2$ and $T \in H_t$ the monomial \mathbf{x}_T is a lexicographic leading monomial for S . Note that $|T| = t$ and $2t - 1 \in T$. The statement is clear for $t = 1$, in fact x_1 is a leading monomial for S , because $a_1x_1 + \dots + a_nx_n - k$ vanishes on S . Suppose for the rest of the proof that $t > 1$.

We employ the Lex game method, proving that Lea wins the the lex game $\text{Lex}(S, \mathbf{v}_T)$, where \mathbf{v}_T is the characteristic vector of T . After Stan specifies

the coordinate values y_{2t}, \dots, y_n , what remains (if Lea has not won yet) is a lex game $\text{Lex}(V, \mathbf{v}_T)$ where $V \subseteq \{0, 1\}^{2t-1}$ defined by $\sum_{i=1}^{2t-1} a_i v_i = k'$, for some positive integer $k' \leq k$, and \mathbf{v}_T is viewed now as a vector in $\{0, 1\}^{2t-1}$.

Let $\mathcal{V} \subseteq 2^{[2t-1]}$ denote the set family whose corresponding set of characteristic vectors is V . We claim that \mathcal{V} does not shatter T . To be more specific, either there is no $F \in \mathcal{V}$ such that $F \cap T = T$, or there is no $G \in \mathcal{V}$ such that $G \cap T = \emptyset$.

Suppose for contradiction that both $F, G \in \mathcal{V}$ exist. Then

$$\sum_{i \in [2t-1] \setminus T} a_i \geq \sum_{i \in G} a_i = k' = \sum_{i \in F} a_i \geq \sum_{i \in T} a_i. \quad (3)$$

But this is in contradiction with the inequality of Lemma 2.2, proving the claim. We obtained that \mathbf{x}_T is a lex leading monomial for V , the corresponding vanishing polynomial being either \mathbf{x}_T or $\prod_{i \in T} (x_i - 1)$. This implies, that Lea wins the game $\text{Lex}(V, \mathbf{v}_T)$, hence also $\text{Lex}(S, \mathbf{v}_T)$ as well. This finishes the proof. \square

Remark. We can exhibit a polynomial $Q(\mathbf{x}) \in \mathbb{Q}[\mathbf{x}]$ vanishing on S with leading term \mathbf{x}_T without using directly the Lex game method, as follows. Let $U_0 \subseteq \{0, 1\}^{n-2t+1}$ denote the set of all vectors (v_{2t}, \dots, v_n) which can be extended into a vector in S which has 0 coordinate values everywhere in T . Let $P(x_{2t}, \dots, x_n) \in \mathbb{Q}[\mathbf{x}]$ be a polynomial which is 0 on U_0 and is 1 on $\{0, 1\}^{n-2t+1} \setminus U_0$. Then set

$$Q(x_1, \dots, x_n) = \prod_{i \in T} (x_i - P(x_{2t}, \dots, x_n)).$$

It is immediate that the lex leading term of Q is \mathbf{x}_T , since $T \subseteq [2t-1]$. Let $\mathbf{v} \in S$ be an arbitrary vector. On one hand, if $\mathbf{u} = (v_{2t}, \dots, v_n) \in U_0$, then $Q(\mathbf{v}) = \prod_{i \in T} v_i = 0$ because by the claim in the preceding proof vectors from U_0 do not have extensions $\mathbf{v} \in S$ with $v_i = 1$ for all $i \in T$. On the other hand, if $\mathbf{u} \in \{0, 1\}^{n-2t+1} \setminus U_0$, then $Q(\mathbf{v}) = \prod_{i \in T} (v_i - 1) = 0$ because \mathbf{u} has no extension $\mathbf{v} \in S$ with values $v_i = 0$ for all $i \in T$. We note also, that using the equality $P^2 = P$ of functions defined on $\{0, 1\}^n$, we have

$$Q(x_1, \dots, x_n) = \mathbf{x}_T + \left(\prod_{i \in T} (x_i - 1) - \mathbf{x}_T \right) P(x_{2t}, \dots, x_n),$$

again an equality of functions on $\{0, 1\}^n$.

Proof of Proposition 1.4. The statement is clear for $t = 1$. For a vector $\mathbf{v} \in S_p(\mathbf{a}, k)$ the value v_1 is determined by the rest of the values v_i because a_1 is not 0 modulo p . Henceforth we assume that $t > 1$. As with Theorem 1.1, it suffices to show that a set $V \subseteq \{0, 1\}^{2t-1}$ defined by $\sum_{i=1}^{2t-1} a_i v_i \equiv k' \pmod{p}$ for some integer $0 \leq k' \leq p-1$, can not shatter T . Assume the contrary. Let $\mathbf{v} = \mathbf{v}^{(0)} \in V$ be a vector which is 0 at every coordinate from T . Also let $\mathbf{u} = \mathbf{v}^{(t)} \in V$ be a vector which has coordinates 1 at every coordinate from T . Using Lemma 2.2 we obtain

$$0 \leq \sum_{i \in [2t-1]} a_i v_i \leq \sum_{i \in [2t-1] \setminus T} a_i < \sum_{i \in T} a_i \leq \sum_{i \in [2t-1]} a_i u_i \leq \sum_{i \in [2t-1]} a_i < 2p.$$

This is possible only if $\sum_i a_i v_i = k'$ and $\sum_i a_i u_i = k' + p$. Now for $\ell = 1, \dots, t-1$ let $\mathbf{v}^{(\ell)} \in V$ be a vector which is 1 in the first ℓ coordinates from T , and is 0 at the remaining $t - \ell$ coordinates belonging to T . It follows from the indirect hypothesis that such vectors $\mathbf{v}^{(\ell)}$ exist. The inequality $\sum_{i \in [2t-1]} a_i < 2p$ implies that for every ℓ the sum $\sum_{i \in [2t-1]} a_i v_i^{(\ell)}$ is either k' or $k' + p$. Clearly there must be an index j with $0 \leq j < t$, such that $\sum_{i \in [2t-1]} a_i v_i^{(j)} = k'$ and $\sum_{i \in [2t-1]} a_i v_i^{(j+1)} = k' + p$. Set $\mathbf{w} = \mathbf{v}^{(j+1)} - \mathbf{v}^{(j)}$. This vector has ± 1 and 0 coordinates, moreover it is 0 on T with the exception of $w_s = 1$, where $s \in [2t-1]$ is the $(j+1)^{\text{th}}$ element of T . Therefore we have

$$p = \sum_{i=1}^{2t-1} a_i w_i \leq a_s + \sum_{i \in [2t-1] \setminus T} a_i \leq a_s + \sum_{i \in T \setminus \{2t-1\}} a_i \leq \sum_{i \in T} a_i < p, \quad (4)$$

a contradiction proving the statement. At the second inequality we used Lemma 2.2 again, and $a_s \leq a_{2t-1}$ at the third. \square

Verification of Example 1. We recall first the following recursion for the lex standard monomials (see the proof of Theorem 4.3 in [2]). Let $V \subseteq \{0, 1\}^n \subseteq \mathbb{F}^n$ be a subset of the Boolean cube. Define the sets of vectors

$$V_0 := \{\mathbf{v} \in \{0, 1\}^{n-1} : (\mathbf{v}, 0) \in V\}$$

and

$$V_1 := \{\mathbf{v} \in \{0, 1\}^{n-1} : (\mathbf{v}, 1) \in V\}.$$

Then for the lex standard monomials of $I(V)$ we have

$$\text{sm}(I(V)) = \text{sm}(I(V_0)) \cup \text{sm}(I(V_1)) \cup \{\mathbf{m}x_n : \mathbf{m} \in \text{sm}(I(V_0)) \cap \text{sm}(I(V_1))\}.$$

We apply this in the case $V := S(\mathbf{a}, k)$, $\mathbf{a} = (1, \dots, 1, t)$. It is easy to see that

$$V_0 = \{(v_1, \dots, v_{n-1}) \in \{0, 1\}^{n-1} : \sum_{i=1}^{n-1} v_i = k\}$$

and

$$V_1 = \{(v_1, \dots, v_{n-1}) \in \{0, 1\}^{n-1} : \sum_{i=1}^{n-1} v_i = k - t\}.$$

Observe that V_0 and V_1 correspond to complete uniform families. Then by the results of Section 2 and Theorem 4.3 of [2] we have

$$\text{sm}(I(V_0)) = \mathcal{M}_{k,n-1}$$

and

$$\text{sm}(I(V_1)) = \mathcal{M}_{k-t,n-1}.$$

These together imply that

$$\begin{aligned} \text{sm}(I(V)) &= \mathcal{M}_{k,n-1} \cup \mathcal{M}_{k-t,n-1} \cup \{\mathbf{m}x_n : \mathbf{m} \in \mathcal{M}_{k,n-1} \cap \mathcal{M}_{k-t,n-1}\} = \\ &= \mathcal{M}_{k,n-1} \cup \{\mathbf{m}x_n : \mathbf{m} \in \mathcal{M}_{k-t,n-1}\}. \end{aligned}$$

Here we used that $0 \leq k - t < k \leq \frac{n-1}{2}$, and hence $\mathcal{M}_{k-t,n-1} \subseteq \mathcal{M}_{k,n-1}$. \square

References

- [1] Adams, W. W., Loustaunau, P.: An Introduction to Gröbner bases. American Mathematical Society (1994)
- [2] Anstee, R.P., Rónyai, L., Sali, A.: Shattering News. Graphs and Combinatorics **18**, 59–73 (2002)
- [3] Babai, L., Frankl, P.: Linear Algebra Methods in Combinatorics with Applications to Geometry and Computer Science. The University of Chicago (1992)
- [4] Balandraud É., Girard B.: A Nullstellensatz for Sequences Over \mathbb{F}_p . Combinatorica **34**, 657–688 (2014)

- [5] Buchberger, B.: Gröbner-Bases: An Algorithmic Method in Polynomial Ideal Theory. In: Bose, N.K. (ed.) Multidimensional Systems Theory - Progress, Directions and Open Problems in Multidimensional Systems Theory. 184-232, Reidel Publishing Company, Dordrecht - Boston - Lancaster (1985)
- [6] Cohen, A.M., Cuypers, H., Sterk, H. (eds.): Some Tapas of Computer Algebra. Springer-Verlag, Berlin, Heidelberg (1999)
- [7] Cox, D., Little, J., O'Shea, D.: Ideals, Varieties, and Algorithms. Springer-Verlag, Berlin, Heidelberg (1992)
- [8] Felszeghy, B., Ráth, B., Rónyai, L.: The lex game and some applications. J. Symbolic Computation **41**, 663–681 (2006)
- [9] Frankl, P.: Traces of antichains. Graphs Comb. **5**, 295–299 (1989)
- [10] Frankl, P.: Intersection Theorems and mod p Rank of Inclusion Matrices. Journal of Combinatorial Theory, Series A. **54**, 85–94 (1990)
- [11] Hegedűs, G., Rónyai, L.: Gröbner bases for complete uniform families. J. of Algebraic Combinatorics **17**, 171–180 (2003)
- [12] Hegedűs, G., Rónyai, L.: Standard Monomials for q -uniform Families and a Conjecture of Babai and Frankl. Central European Journal of Mathematics. **1**, 198–207 (2003)
- [13] Lovász, L.: Combinatorial Problems and Exercises. Akadémiai Kiadó, Budapest (1979)
- [14] Rónyai, L., Mészáros, T.: Some combinatorial applications of Gröbner bases. In: Algebraic Informatics (Winkler, F. ed.), 4th International Conference, CAI 2011, Linz, Proceedings. 65–83, Springer-Verlag, Heidelberg (2011)